

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10177552 A**

(43) Date of publication of application: **30 . 06 . 98**

(51) Int. Cl

G06F 15/00

G06F 1/00

G06F 13/00

(21) Application number: **08337260**

(71) Applicant: **FUJI XEROX CO LTD**

(22) Date of filing: **17 . 12 . 96**

(72) Inventor: **YAMAGUCHI YASUICHIROU**

(54) **AUTHENTICATION ANSWER METHOD AND
AUTHENTICATION ANSWER DEVICE USING THE
ANSWER METHOD**

information requested by the server 1 to this server in
place of the client C.

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To secure the quick operability, to reduce the communication frequency and to attain the use of a terminal of the light specifications such as a PDA, etc., in the communication requiring the authentication information by returning the authentication information requested by a server to this server in place of a client when this client gives an access request to the server.

SOLUTION: This device consists of a client C of a PDA serving as a user terminal, a substitute server which serves as an authentication answer device and a server S which offers various services. The substitute server includes an authentication answer management part which totally controls an authentication answer. In such a constitution, the authentication answer management part collectively manages the authentication information necessary for every server when the client C has an access to the server S. When the client C has an access request to a server S1, for example, the authentication answer management part returns the authentication



This Page Blank (uspto)

②

類似技術

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-177552

(43) 公開日 平成10年(1998) 6月30日

(51) Int.Cl. ⁸	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 C
1/00	3 7 0	1/00 3 7 0 E
13/00	3 5 7	13/00 3 5 7 Z

審査請求 未請求 請求項の数 9 O L (全 9 頁)

(21) 出願番号 特願平8-337260

(22) 出願日 平成 8 年(1996) 12月17日

(71) 出願人 000005496

富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72) 発明者 山口 保一郎

神奈川県川崎市高津区坂戸 3 丁目 2 番 1 号
K S P R & D ビジネスパークビル 宮
士ゼロックス株式会社内

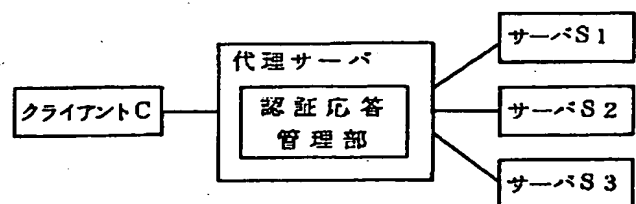
(74) 代理人 弁理士 吉田 研二 (外 2 名)

(54) 【発明の名称】 認証応答方法およびその方法を用いた認証応答装置

(57) 【要約】

【課題】 複数のサーバにアクセスするとき、それぞれ認証作業が必要だった。これを鍵束のような機構でユーザ端末で管理しても、通信回数が多く、処理の負荷も軽くなかった。

【解決手段】 クライアント C と複数のサーバ S 1 等の間に代理サーバを設ける。この代理サーバは認証応答管理部をもつ。認証応答管理部は、自身がクライアントを認証し、いったん認証したクライアントについて、複数のサーバに対する認証情報の応答を代行する。



特定コンソールのみに認証により
制限する。

【特許請求の範囲】

サーバ側

【請求項1】 クライアントからサーバにアクセスするときにサーバごとに必要となる認証情報を一括して管理しておき、クライアントからあるサーバに対するアクセスが要求されたとき、そのクライアントの代わりにそのサーバが求める認証情報をそのサーバに返すことを特徴とする認証応答方法。

【請求項2】 サーバクライアントシステムにおいてクライアントと複数のサーバを中継する装置であって、複数のサーバに対するクライアントの認証情報を保持する保持手段と、

クライアントからあるサーバに対するアクセスの要求があったとき、保持手段からそのサーバに関する認証情報を読み出す読出手段と、

を含み、クライアントに代わってサーバに認証応答をすることを特徴とする認証応答装置。

【請求項3】 該装置自身がクライアントを認証する手段をさらに含み、クライアントが該装置に対して適正な認証情報を返したときに限り、以降クライアントに代わってサーバに認証応答する請求項2に記載の認証応答装置。

【請求項4】 該装置自身がクライアントを認証する手段と、

クライアントが該装置に対して適正な認証情報を返したとき、前記読出手段による読出を許可する許可手段と、をさらに含み、読み出された認証情報をクライアントに代わってサーバに返す請求項2に記載の認証応答装置。

【請求項5】 所定の条件に従って前記読出手段による読出を禁止する禁止手段をさらに含む請求項4に記載の認証応答装置。

【請求項6】 クライアントから新たなサーバに対するアクセスの要求があったとき、クライアントから送信された該サーバに対する認証情報を前記保持手段に追加登録する登録手段をさらに含む請求項2～5のいずれかに記載の認証応答装置。

【請求項7】 サーバクライアントシステムにおいてクライアントと複数のサーバを中継する装置であって、クライアントに対してサーバとして振る舞うサーバ部と、

サーバに対してクライアントとして振る舞うクライアント部と、

クライアントがサーバにアクセスする際、サーバごとに必要となる認証情報を一括して保持するテーブルとを含み、

前記サーバ部は、

この装置自身がクライアントを認証するための認証手段と、

この認証手段によってクライアントが認証されたとき、このクライアントに関して前記テーブルの読出を許可する許可手段とを含み、

前記クライアント部は、

クライアントからあるサーバへのアクセス要求があったとき、このクライアントに関してテーブルの読出が許可されていれば、そのサーバに対する認証情報を読み出す読出手段と、

読み出された認証情報を前記サーバへ送る通信手段と、を含むことを特徴とする認証応答装置。

【請求項8】 前記サーバ部は、クライアントから新たなサーバに対するアクセス要求があったとき、クライアントから送信された該サーバに対する認証情報を前記テーブルに追加登録する登録手段をさらに含む請求項7に記載の認証応答装置。

【請求項9】 前記サーバ部は、所定の条件に従って前記読出手段による読出を禁止する禁止手段をさらに含む請求項8に記載の認証応答装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、認証応答方法および装置、特に、サーバクライアントシステムにおいてサーバとクライアント間を中継し、サーバの認証要求に対して応答する方法および装置に関する。

【0002】

【従来の技術】例えばインターネットなどのオープンネットワークでは、フリー（無料）の情報公開がひとつの原則になっている。この原則により、より多くのユーザがより有用な情報に自由にアクセスできる環境が整備、強化されつつある。しかしその一方、例えば契約したユーザのみに特定のサービスを提供したい場合には、サービス提供者と契約者の間で一定のセキュリティ関係を構築する必要がある。この最も簡単な例は、契約者にユーザ名とパスワードなどの認証情報を割り当て、サービスにアクセスする際、これらを入力させる方法である。

【0003】例えばインターネットでサービスの提供を受ける場合、ユーザはまず画面で所望のサービスを選択する。この要求はサーバに伝えられる。もしそのサーバが、サービスの提供に当たってユーザの認証を行うサーバである場合、ユーザ端末のクライアントに対して認証情報の問合せがなされる。ユーザが認証情報を入力すればこれがサーバに返され、この認証情報が正しければユーザの求めるサービスが提供される。インターネットの利点のひとつは、ユーザがいろいろなサーバから異なるサービスを容易に受けられる点にある。ただしこの場合、通常サーバどうしは互いに独立しているため、サーバごとにクライアントに対して認証情報の入力を要求してくる。

【0004】図7は、従来のサーバクライアントシステムにおいて、クライアントから異なる2つのサーバに要求が発せられる様子を示している。同図のごとく、まず始めにクライアントCからサーバS1に要求が出される(T1)。サーバS1は認証情報を求めるサーバであ

り、クライアントにその旨の問合せがなされる(T2)。クライアントはサーバS1のための認証情報(ユーザ名U1とパスワードP1)をもって応答する(T3)。このとき、一般的なブラウザ(情報端末に搭載された情報可視化プログラム、またはそれを搭載した端末)は、認証情報U1/P1を自己のバッファに記憶しておく。一方、サーバS1は認証情報U1/P1を検査し、それらが正しければ、求められたサービスをクライアントに提供する(T4)。

【0005】つづいて、クライアントCが別のサーバS2にサービスを要求する(T5)。サーバが変わったことは、ユーザは特に意識しない。要求の送付にあたり、ブラウザはバッファに記憶していた認証情報U1/P1をサーバ名S2に付して送付する。この認証情報はサーバS1に対するものであってサーバS2にとっては適正ではないため、サーバS2から独自に認証情報の問合せがなされる(T6)。クライアントはサーバS2のための認証情報U2/P2を入力しなおして応答する(T7)。サーバS2は認証情報U2/P2の確認後、クライアントにサービスを提供する(T8)。

【0006】以上、このシステムでは、サーバが変わるたびに認証情報の問合せと入力が必要になる。この煩わしさを回避するために、「Macintosh漢字Talk 7.5、アップグレードガイド」のp22~26に、単一のパスワードによってネットワーク上の複数のサービスが受けられる「鍵束」という機能が説明されている。すなわち、サービスごとに異なる鍵を束の状態に管理し、この鍵束に対して固有のパスワードを設けるといもので、このパスワードを入れさえすればサービスに応じて必要な鍵が鍵束から選択され、これがサーバに渡される。

【0007】

【発明が解決しようとする課題】上述の鍵束に関する機能はユーザの端末に搭載されるソフトウェアで実現される。この従来技術の場合、以下の点で改善の余地が認められる。

【0008】1. ユーザがパスワードを入れる回数は減るが、クライアントとサーバ間の通信回数が減らない。例えば、図7の一連の通信において、T3とT7における認証情報のユーザによる入力なくなるが、問合せと応答自体は必要であり、図7と同じ通信回数になる。このため、通信コストの低減に結びつかないだけでなく、サービスの迅速性が阻害される。

【0009】2. ユーザの端末がPDA(Personal Digital Assistance)など比較的軽いハードウェア仕様である場合、複数のサーバに対するアクセスを管理し、実行する一連の処理の負荷が重い。このため、処理の即時性に欠けることがある。

【0010】3. 鍵束の機能を実現するために、ユーザの端末に手を加えなければならない。

【0011】本発明は以上の課題に鑑みてなされたものであり、その目的は、認証情報を必要とする通信における迅速性を確保し、通信回数を低減し、PDAなど軽い仕様の端末でも実現可能であり、その端末に手を加える必要のない認証応答方法および装置を提供することにある。

【0012】

【課題を解決するための手段】本発明の認証応答方法は、クライアントからサーバにアクセスするときにサーバごとに必要となる認証情報を一括して管理しておき、クライアントからあるサーバに対するアクセスが要求されたとき、そのクライアントの代わりにそのサーバが求める認証情報をそのサーバに返すものである。この方法によれば、認証情報の問合せと応答がクライアントとサーバ間ではなく、認証情報の管理主体とサーバ間に発生する。このため、クライアントは応答の義務から開放され、通信回数が減る。また、クライアントが応答しなくてよいため、PDAなど、軽い仕様の端末で処理上なんら問題は生じない。端末に新たな機能を追加する必要もなく、管理主体に認証情報の一括管理機能を設ければ足りる。

【0013】一方、本発明の認証応答装置は、サーバクライアントシステムにおいてクライアントと複数のサーバを中継する装置である。この装置は、複数のサーバに対するクライアントの認証情報を保持する保持手段(20)と、クライアントからあるサーバに対するアクセスの要求があったとき、保持手段からそのサーバに関する認証情報を読み出す読出手段(36)とを含み、クライアントに代わってサーバに認証応答をする。この装置では、クライアントの認証情報が保持手段に記憶されているため、クライアントが例えばサーバS1にアクセスしたければ、読出手段が保持手段からこのクライアントのサーバS1に関する認証情報(例えばU1/P1)を読み出す。つづいてこれをサーバS1に送る。このため、クライアントは認証応答から開放され、上述の認証応答方法同様の効果が得られる。

【0014】本発明の認証応答装置はさらに、この装置自身がクライアントを認証する手段(32)と、クライアントが該装置に対して適正な認証情報を返したとき、前記読出手段による読出を許可する許可手段(34)とを含んでもよい。つまり、サーバS1などへのアクセスに先立ち、この装置が自らクライアントを認証する。ここで正しい認証情報が入力されれば、以降、サーバS1等に対する認証応答を代行する。この構成によれば、ユーザは認証情報を管理する装置があることを知り、これを積極的に活用することができる。

【0015】本発明の認証応答装置はさらに、所定の条件に従って前記読出手段による読出を禁止する禁止手段(38)を含んでもよい。この構成によれば、例えば一定期間ごとに読出を禁止することにより、セキュリティ

読出許可状態にあるか否かを検査する許否検査部48を含む。

【0027】図3はテーブル20の詳細を示す構成図である。同図のごとくテーブル20は、クライアントごと、すなわちユーザU0～Unに分割された複数のブロック70の集合体である。各ブロック70には、U0等のユーザ名72、そのブロック70の読出の許可、禁止状態をそれぞれ「○」「×」で示す許否フラグ74、サーバ名76、認証情報78の各領域をもつ。例えばユーザU0の場合、サーバS0等に対する認証情報がU00/P00等と記憶されている。ユーザU0のブロックの許否フラグは「○」であり、テーブル20において、少なくともこのユーザのブロック70は読出許可状態にあることがわかる。許否フラグ74は初期状態ではすべて「×」である。以下、ユーザU0がいろいろなサーバへアクセスする際の代理サーバの動作を説明する。

【0028】1. 認証情報が記憶されている複数サーバへの連続アクセス

図4はクライアントCに当たるユーザU0がサーバS1、S2に対してつづけてアクセスする通信の手順を示している。同図のごとく、まず始めにクライアントCから代理サーバS0に対して、「サーバS1にアクセスしたい」旨の要求が送出される(T1)。この要求は、クライアントCを特定する「U0」および目的のサーバS1を特定する「S1」の2つのパラメータで構成される。これらのパラメータは図2の第一通信部12を介してサーバ部16の受付部30で受け取られ、クライアント部18の読出制御部36へ送られる。このとき、パラメータには認証情報(U00/P00等)が含まれていないため、認証部32は動作しない。

【0029】読出制御部36の検索部46は、ユーザ名であるU0をキーとしてテーブル20に検索をかける。その結果、図3の最も左側のブロックが発見される。つづいて許否検査部48がそのブロックの許否フラグ74の状態を確かめる。この場合、まだ初期状態で「×」であるから、「読出は禁止」と判断される。このため目的のサーバS1が必要とする認証情報を読み出すことはできず、代理サーバS0としては、まずこのユーザU0を自装置で認証する必要があること知る。そこで、読出制御部36は切替部54に対し、

「代理サーバS0に対する認証情報を入力してください」

というメッセージを送る。切替部54はこのメッセージを第一通信部12を介してクライアントCへ送り、認証情報を問い合わせる(T2)。クライアントCは端末の画面にこのメッセージを表示し、ユーザは代理サーバS0に対する自己の認証情報「U00/P00」を入力する。この認証情報は、すでに判明している目的サーバ名「S1」と組み合わせられ、第一通信部12を介して受付部30に送られ、認証部32へ回送される(T3の前

半)。

【0030】認証部32では、まず登録指示検出部42がこのパラメータ「S1/U00/P00」を判読する。この場合、S1は新たなサーバではないため、登録の指示ではないと判断され、登録部40は動作しない。つづいて認証検査部44が、パラメータU00/P00をテーブル20に照合し、代理サーバS0に対するユーザU0の正しい認証情報であるか否かを確認する。U00/P00はテーブル20のユーザU0用ブロックのサーバS0に対する認証情報と一致するため、「正しい」旨が読出許可部34に通知される。読出許可部34は、ユーザU0のブロック70の許否フラグ74を「×」から「○」に変更し、以降の読出を許可する。なお、代理サーバS0に対する誤った認証情報が入力された場合は、入力部32から「もういちど入力してください」などのエラーメッセージが切替部54に送られ、これがクライアントCに送付される。

【0031】つぎに、読出制御部36の検索部46がユーザU0のブロック70を検索し、許否検査部48がそのブロック70の許否フラグ74を検査する。ここでは「○」に変更されているため、目的サーバ名「S1」に対応する認証情報「U01/P01」が読み出される。このとき、許否フラグが確実に「○」に変更されるまで検査を待たせる趣旨で、必要に応じて検査を遅延させてもよい。読み出されたパラメータ「U01/P01」はクライアント部18の送出部60に送られ、第二通信部14を介してサーバS1にアクセス要求として送り出される(T3の後半)。

【0032】サーバS1では、ユーザU0からの最初のアクセスであるにも拘らず必要な認証情報が正しく与えられたため、認証情報の問合せをスキップし、要求されたサービスを提供する。サービスを実現するデータは第二通信部14を経てクライアント部18の受付部62で受け取られ、切替部54に向けて出力される。切替部54はこのデータを第一通信部12を介してクライアントCへ送付する(T4)。以上が最初のサーバに対するアクセスである。

【0033】つづいてクライアントCは、代理サーバS0に対し、別のサーバS2に対するアクセスの要求を送る(T5の前半)。この要求はクライアントCを特定する「U0」と目的のサーバを特定する「S2」の2つのパラメータで構成される。これらのパラメータはサーバ部16の受付部30からクライアント部18の読出制御部36へ送られる。このときもパラメータに認証情報が含まれていないため、認証部32は動作しない。読出制御部36の検索部46はユーザU0用のブロック70を見つけ、許否検査部48が許否フラグ74の状態を確かめる。この場合、すでに「○」、すなわち読出許可状態にあるため、目的サーバ名「S2」に対応する認証情報「U02/P02」が読み出される。このパラメータは

のレベルを初期状態に戻すことができる。

【0016】本発明の認証応答装置はさらに、クライアントから新たなサーバに対するアクセス要求があったとき、クライアントから送信された該サーバに対する認証情報を前記保持手段に追加登録する登録手段(40)を含んでもよい。新たなサーバについて、保持手段はそのサーバ用の認証情報をもっていない。したがって、クライアントは認証情報を入力せざるを得ず、これがサーバに伝えられる。このとき、この認証情報を捕捉して保持手段に書き込んでしまうのである。この構成によれば、保持手段の保守作業の労力を軽減することができる。

【0017】本発明の認証応答装置の別の態様は、クライアントに対してサーバとして振る舞うサーバ部(16)と、サーバに対してクライアントとして振る舞うクライアント部(18)と、クライアントがサーバにアクセスする際、サーバごとに必要となる認証情報を一括して保持するテーブル(20)とを含み、前記サーバ部は、この装置自身がクライアントを認証するための認証手段(32)と、この認証手段によってクライアントが認証されたとき、このクライアントに関して前記テーブルの読出を許可する許可手段(34)とを含み、前記クライアント部は、クライアントからあるサーバへのアクセス要求があったとき、このクライアントに関してテーブルの読出が許可されていれば、そのサーバに対する認証情報を読み出す読出手段(36)と、読み出された認証情報をサーバに送る通信手段(14)とを含む。

【0018】この構成において、サーバ部の認証手段がまずクライアントを認証する。認証の後、許可手段により、そのクライアントに関してテーブルの読出が許可される。この後、このクライアントからあるサーバへのアクセス要求があったとき、読出手段によって、そのサーバに対する認証情報が読み出される。読み出された認証情報はサーバに送られる。このため、上述の認証応答方法同様の効果が得られる。

【0019】

【発明の実施の形態】本発明の好適な実施形態を適宜図面を参照しながら説明する。以下、認証情報はユーザ名とパスワードで構成されるものとし、前者をU、後者をPと総括的に表記する。同様にサーバをSと表記し、ユーザU_iのサーバS_jに対する正しい認証情報は、U_i / P_jであるとする。添え字は説明上必要なときに付する。

【0020】図1は本発明の認証応答装置を用いるシステムの概念的な構成図である。同図のごとくこのシステムは、ユーザの端末であるPDAのクライアントCと、認証応答装置である代理(プロキシ)サーバと、各種サービスを提供するサーバSからなる。代理サーバは認証応答全般を司る認証応答管理部を含む。代理サーバは便宜上サーバS₀とし、クライアントCはユーザU₀であるとする。したがって、このクライアントCの代理サ

ーバに対する認証情報は、U₀₀/P₀₀である。なお、同図ではクライアントCがひとつしか存在しないが、実際には多数存在することが考えられる。

【0021】この構成において、認証応答管理部は、クライアントCがサーバSにアクセスするときサーバごとに必要となる認証情報を一括して管理している。クライアントCからあるサーバへのアクセスが要求されたとき、認証応答管理部はクライアントCに代わってそのサーバが求める認証情報をそのサーバに返す。

【0022】図2は代理サーバの内部構成を示す。代理サーバは、クライアントCと要求および応答を通信する第一通信部12、認証応答管理部10、サーバSと要求および応答を通信する第二通信部14を含む。

【0023】認証応答管理部10は、クライアントCからサーバに見えるサーバ部16と、サーバSからクライアントに見えるクライアント部18と、認証情報をクライアント別に記憶するテーブル20を含む。

【0024】サーバ部16は、第一通信部12を介してクライアントCからの送信内容を受ける受付部30と、代理サーバが自己のためにクライアントCを認証する認証部32と、認証部32の認証結果にもとづき、テーブル20からの読出をクライアントごとに許可する読出許可部34と、所定の条件にしたがってテーブル20からの読出を禁止する読出禁止部38と、クライアントCから新たなサーバに対するアクセスが要求されたとき、そのサーバに必要な認証情報をクライアントCの送信内容から抽出してテーブル20に追加登録する登録部40と、3つの方向、すなわち認証部32、後述のクライアント部18の読出制御部36およびクライアント部18の受付部62からのメッセージ等のデータを切り替えて第一通信部12へ送り出す切替部54を含む。登録部40における登録のためには、ユーザ名の他に、当然ながら目的のサーバに対するそのユーザの認証情報が必要である。

【0025】認証部32は、クライアントCからの送信内容がテーブル20に対する新たな認証情報の登録を指示しているか否かを検査する登録指示検出部42と、テーブル20を走査してクライアントCの代理サーバに対する認証情報が正しいか否かを検査する認証検査部44を含む。読出禁止部38は、クライアントごとに禁止条件が満たされているか否かを確認する禁止管理部50と、その指示によってクライアントごとに読出を禁止する個別読出禁止部52を含む。

【0026】一方、クライアント部18は、実際にテーブル20からの読出を制御する読出制御部36と、読み出されたデータを受け付け、これを第二通信部14に送る送出部60と、サーバSから第二通信部14を介してその送信内容を受ける受付部62を含む。読出制御部36はさらに、読み出すべきクライアントのデータを検索する検索部46と、そのクライアントに関するデータが

クライアント部18の送出部60に送られ、第二通信部14を介してサーバS1にアクセス要求として送り出される(T5の後半)。以下、サーバS2によるサービスの提供(T6)はT4同様である。

【0034】なお、セキュリティを考えた場合、いったん読出許可状態になったブロック70が以降無条件でその状態を保つことは望ましくない。このため、読出禁止部38は読出許可状態にあるブロックを再度禁止状態にもどす。禁止管理部50は禁止状態にもどすための条件を管理しており、例えば一連のセッションが終了したときや、一定期間クライアントからサーバへのアクセスがない場合など、ある条件が満たされたとき、禁止すべきブロック70を個別読出禁止部52へ通知する。個別読出禁止部52は、通知されたブロック70の許否フラグ74を「○」から「×」に戻す。

【0035】以上、本実施の形態によれば、図7の通信手順に比べてクライアントCとサーバS1、S2の通信回数を減らすことができる。これは代理サーバS0がサーバS1、S2に代わってクライアントの認証を行い、クライアントに代わってサーバS1、S2への認証応答を行うためである。また本実施の形態によれば、異なる認証情報が一括管理、応答されるため、サーバが変わるたびにユーザがいちいち認証情報を入れなおす必要がなくなる。例えば図4の場合、以降クライアントCがサーバS1、S2を交互にアクセスするときでも、もはや認証情報の入力はいっさい不要である。このため、さらに図7の場合との差が大きくなる。本実施の形態では、ユーザの端末であるPDAなどで鍵束を管理する必要がなく、端末側の処理負荷が軽くなる。また、代理サーバのみに手を加えればよいので、既存のサーバやクライアントに変更もいらない。代理サーバひとつで多数のクライアント、サーバをカバーできるため、本実施の形態は実施の際も効率的である。

【0036】2. 認証情報の不要なサーバへのアクセス
サーバの中には認証情報を求めないものも多数存在する。そうしたサーバへのアクセスを図5によって説明する。同図において、ユーザU0はサーバS3へアクセスしたいとする。アクセスの要求(T1)、代理サーバS0からの認証情報の問合せ(T2)、それに対する応答(T3の前半)までは図4同等である。応答の結果、認証情報「U00/P00」と目的サーバ名「S3」が組み合わされ、認証部32へ送られる。

【0037】認証部32は、パラメータU00/P00が正しい認証情報であるため、ユーザU0のブロックの許否フラグ74を「×」から「○」に変更する。つぎに読出制御部36は、ユーザU0のブロック70が読出許可状態にあることを知り、目的サーバ名「S3」に対応する認証情報を読み出そうとする。しかし、図3のごとくユーザU0のブロック70にはサーバS3の名前がない。この状況は、

(1) 認証情報の必要な新たなサーバに対するアクセス
(2) 認証情報の不要な新たなサーバに対するアクセス
のいずれかが発生していることを意味する。(1)の場合はクライアントに認証情報を問合せなければならない。しかし、(2)の場合は不要であり、問合せはシステムの動作として不適切である。そこで読出制御部36は、まず(2)を想定し、読出の結果として形式的に「無(null)」を送出部60に送る。したがって、第二通信部14からサーバS3にはアクセスの要求のみが送り出される(T3の後半)。一方、サーバS3は要求があってもユーザの認証を行わないため、無条件でサービスを提供する(T4)。

【0038】以上が認証情報を求めないサーバへのアクセスである。ここでは、まずT2において代理サーバS0自身がユーザの認証を行ったが、別の手順もある。例えば、サーバS3に対するアクセス要求を認証情報の有無に関係なく直接サーバS3に送ってもよい。その場合、要求に対してサーバS3がサービスを提供するという単純な通信手順で済む。この方法の場合、目的のサーバが認証情報を求めるサーバであれば、そのサーバがユーザ名とパスワードの入力を求めてくることになる。そのときに代理サーバが自己に対する認証情報の送付をクライアントに対して求める構成としてもよい。

【0039】3. 認証情報が必要だが未登録のサーバへのアクセス

テーブル20に登録されていない新たなサーバであり、しかもそのサーバが認証情報を要求する場合がある。図6はそうした場合の通信手順を示している。

【0040】同図において、ユーザU0はサーバS3へアクセスしたいとする。アクセスの要求(T1)、代理サーバS0からの認証情報の問合せ(T2)、それに対する応答(T3の前半)、パラメータS3に基づくサーバS3への要求(T3の後半)については図5同等である。要求を受けたサーバS3には、自己が必要とする認証情報が与えられないため、認証情報の問合せを行う(T4)。

【0041】この問合せに対し、ユーザがサーバS3のための認証情報U03/P03を入力する。この認証情報は代理サーバの認証部32へ与えられる。認証部32の登録指示検出部42は、新たなサーバ名が認証情報を伴う形で送られてきたことを確認し、これを新たな登録の指示とみなして登録部40にパラメータS3/U03/P03を送る。登録部40は、テーブル20のユーザU0のブロックに新たなサーバS3の欄を設け、認証情報U03/P03を書き込む。以上が登録動作である。

【0042】一方、読出制御部36はサーバ名「S3」をキーとして認証情報U03/P03を読み出し、これをクライアント部18等を介してサーバS3に送る(T5の後半)。サーバS3は正しい認証情報が与えられことを確認し、求められたサービスを提供する(T6)。

【0043】以上がサーバの登録を伴う通信である。この方法によれば、ユーザが新たなサービスを受けるようになったとき、そのための認証情報を自動的にテーブル20へ追加していくことができる。その結果、テーブル保守の作業工数を大幅に軽減することができる。

【図面の簡単な説明】

【図1】 本発明の認証応答装置を用いるシステムの概念的な構成図である。

【図2】 実施の形態の代理サーバの内部構成図である。

【図3】 図2のテーブルの詳細を示す構成図である。

【図4】 ユーザU0がサーバS1、S2に対してつづけてアクセスする通信の手順を示す図である。

【図5】 認証情報を求めないサーバへのアクセスの通信手順を示す図である。

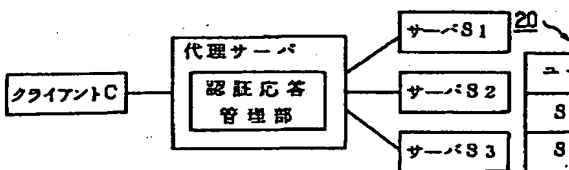
【図6】 認証情報が必要だが未登録のサーバへのアクセスの通信手順を示す図である。

【図7】 従来のサーバクライアントシステムにおいて、クライアントから異なる2つのサーバがアクセスされる様子を示す図である。

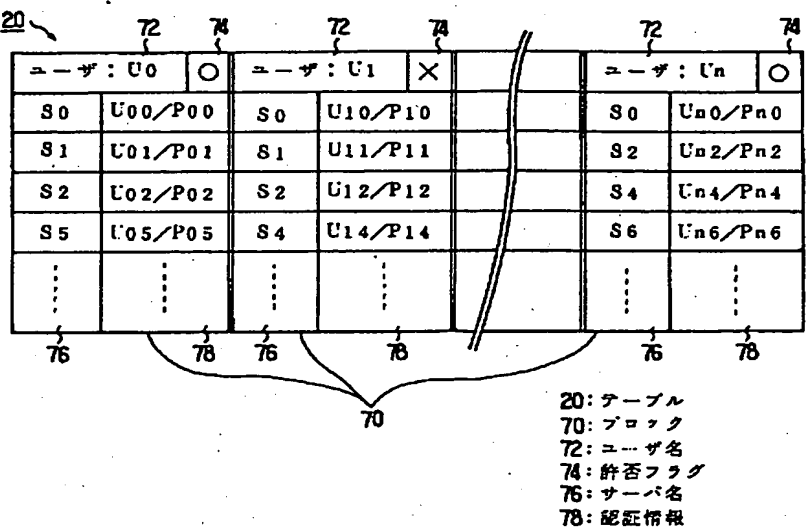
【符号の説明】

10 認証応答管理部、12 第一通信部、14 第二通信部、16 サーバ部、18 クライアント部、20 テーブル、30 受付部、32 認証部、34 読出部、36 読出制御部、38 読出禁止部、40 登録部、42 登録指示検出部、44 認証検査部、46 検索部、48 許可検査部、50 禁止管理部、52 個別読出禁止部、60 送出部、62 受付部、70 ブロック、72 ユーザ名、74 許可フラグ、76 サーバ名、78 認証情報。

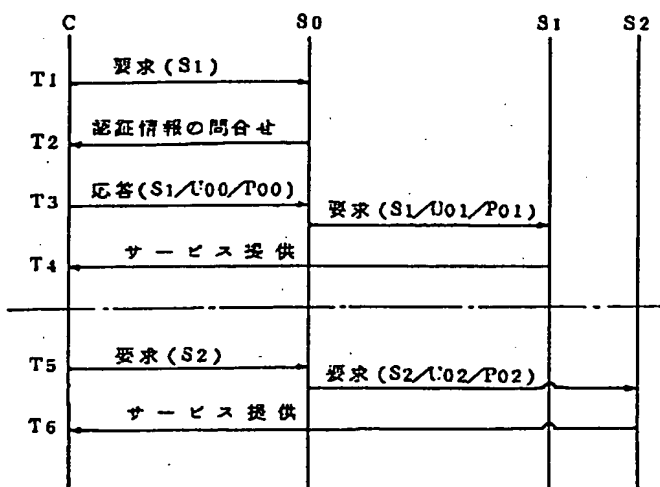
【図1】



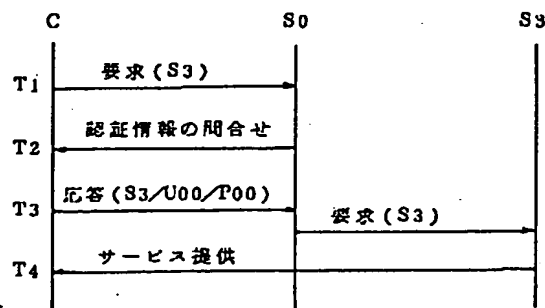
【図3】



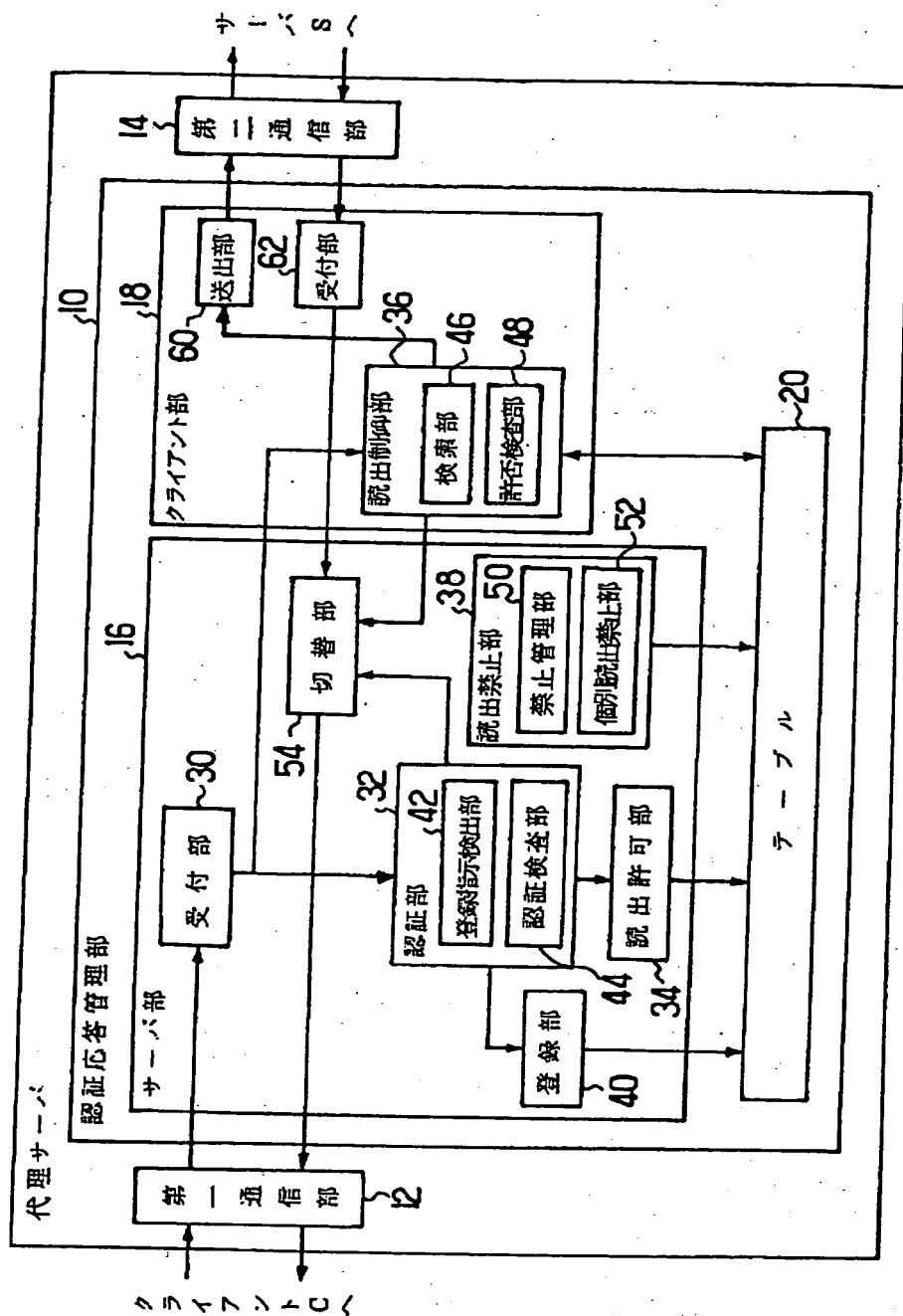
【図4】



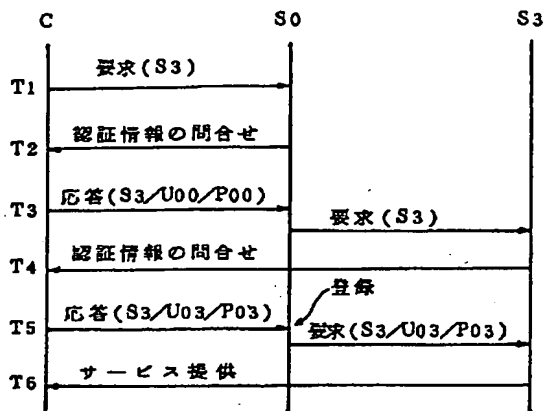
【図5】



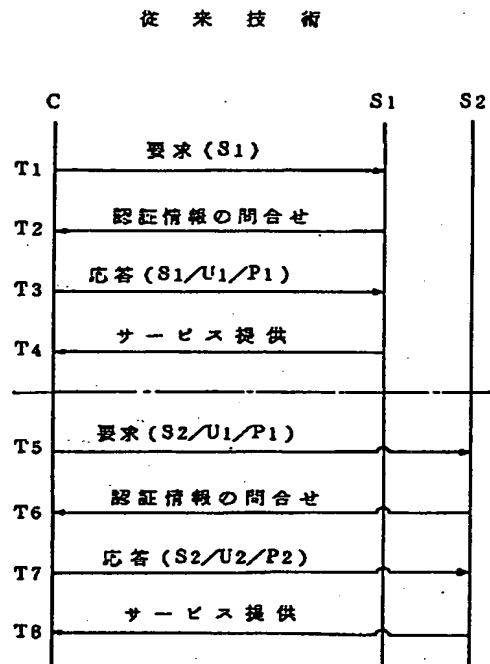
【图 2】



【図6】



【図7】



This Page Blank (usptc)